Application No. 09/670,424   Customer No. 01933
Amendment filed with RCE

Listing of Claims:

Claims 1-29 (Canceled).

30.   (Currently Amended) A database management apparatus
comprising:

a database storage unit which stores a database comprising a
plurality of records, each record including a plurality of data

5   segments identified by ~~respective~~ item <u>category</u> titles <u>that</u>
<u>identify respective categories of the data segments</u>;

an item <u>category</u> title memory for storing at least one item
<u>category</u> title for specifying a corresponding at least one data
segment group as a target of a data search process;

10   a key data memory for storing keys for use in encryption
associated with the database, wherein the keys comprise a column
key corresponding to the at least one data segment group
specified by the at least one stored item <u>category</u> title, and a
plurality of different row keys corresponding respectively to the

15   records of the database; and

an encryption unit for encrypting: (i) the data segments of
said at least one specified data segment group that is the target
of the data search process using the column key corresponding to
the at least one specified data segment group, and (ii) data

-3-

Application No. 09/670,424   Customer No. 01933
Amendment filed with RCE

20   segments of at least one data segment group corresponding to item

category titles other than the stored item ~~titles~~ category title,

in units corresponding to the records, using the different row

keys of the respective records.

     31.   (Previously Presented) The apparatus according to

claim 30, further comprising:

     a functional unit which encrypts a received data set

comprising a search process condition using the corresponding

5   column key; and

     ·a database search unit which performs the data search

process by comparing the encrypted search process condition with

the encrypted data segments of said at least one specified group.

     32.   (Previously Presented) The apparatus according to

claim 30, wherein the encryption unit sequentially generates

vectors in a multidimensional space based on a set of

predetermined functions, and the data segments are encrypted in

5   accordance with an encryption method in which components of the

sequentially generated vectors form a key stream of a key

associated with the encryption method, and

     wherein the row keys and the column key specify constants of

the functions.

                              -4-

33.   (Currently Amended) A database system comprising a

first information processor terminal storing a database, and a

second information processor terminal which is connected to the

first information processor terminal via a network and which is

5   adapted to send a request to the first information processor

terminal for conducting a search process in the database, wherein

the first information processor terminal comprises:

        a functional unit which encrypts: (i) data segments

forming data segment groups corresponding to column item <u>category</u>

10   titles of a first kind using a same column key for said data

segments forming the data segment groups and, (ii) data segments

forming data segment groups corresponding to column item <u>category</u>

titles of a second kind, in units of rows of data segments, using

respective row keys<u>, said item category titles identifying</u>

15   <u>respective categories of the data segments</u>;

        wherein the second information processor terminal comprises:

        a transmitting unit which transfers via the network

[[,]] an encrypted data set representing conditions to be used

for the search process in the first information processor

20   terminal, when the second information processor terminal requests

the first information processor terminal to perform the search

process on the database, said encrypted data set being formed by

encrypting an input data set specifying the conditions of the

search process by using the column key; and

-5-

25   wherein the first information processor terminal further

comprises:

         a search performing unit that performs the search

process on the encrypted database, based on the transmitted

encrypted data set; and

30   a returning unit that returns an encrypted result data

set resulting from the search process, to the second information

processing terminal via the network.

         34.   (Currently Amended) A database management apparatus

comprising:

         a key specification memory for storing data specifying a

type of encryption system to be used to encrypt data segments of

5   each column of a database, if the column of the database is to be

encrypted;

         a first encryption unit that encrypts in accordance with the

data stored in the key specification memory: (i) data segments

forming data segment groups corresponding to column item category

10   titles of a first kind using a same column key for said data

segments forming the data segment groups, and (ii) data segments

forming data segment groups corresponding to column item category

titles of a second kind, in units of rows of the database, using

row keys respectively specified for each of the rows, said item

-6-

Application No. 09/670,424   Customer No. 01933
Amendment filed with RCF

15   <u>category titles identifying respective categories of the data</u>

      <u>segments;</u>

           a second encryption unit that encrypts, using a basic key,

      all of the row keys used by the first encryption unit;

           a key data generating unit that generates the column key,

20   the row keys and the basic key; and

           a storing operation unit which stores in a memory the

      database after encryption by the first encryption unit and the

      row keys after encryption by the second encryption unit, in a

      mutually associated manner.

           35.   (Previously Presented) The apparatus according to

      claim 34, wherein the row keys are each generated based on a

      number of the respective rows and a random number.

           36.   (Previously Presented) The apparatus according to

      claim 34, wherein a vector generation unit sequentially generates

      vectors confined to a closed subspace of an n-dimensional space

      and defined by functions based on the keys; and

5   wherein a logical operation unit performs a logical

      operation in units of a bit involving both the data segments of

      the database and components of the vectors generated by the

      vector generation unit, to encrypt the data segments.

                                  -7-

37. (Currently Amended) A method for managing a database
system including a first terminal unit for managing the database
and a second terminal unit for searching the database
independently of the first terminal unit, said method comprising:

5   encrypting the database by encrypting, on a first terminal
side of the system: (i) data segments forming data segment groups
corresponding to column item category titles of a first kind
using a same column key for said data segments forming the data
segment groups, (ii) data segments forming data segment groups

10   corresponding to column item category titles of a second kind, in
units of rows of the database, using row keys respectively
specified for each of the rows, and (iii) all of the row keys,
using another key, said item category titles identifying
respective categories of the data segments;

15   storing, at the first terminal unit side of the system, the
encrypted database on portable storage medium units for
distribution; and

        searching the encrypted database stored on any of the
distributed storage medium units, decrypting a data set obtained

20   as a search result, and displaying the decrypted data set at a
second terminal unit side of the system.

38. (Previously Presented) The database management method
according to claim 37, wherein each of the storage medium units

-8-

stores both the encrypted database generated by the first

terminal unit, and a predetermined application program for

5   performing a searching process on the encrypted database.

39.   (Currently Amended) A computer-readable storage medium

with a program stored thereon for directing a computer to:

encrypt, in a first mode, data segments forming data segment

groups corresponding to column item <u>category</u> titles of a first

5   kind using a same column key for said data segments forming the

data segment groups, said data segments being elements of a

database;

encrypt, in a second mode, data segments forming data

segment groups corresponding to column item <u>category</u> titles of a

10   second kind using respective row keys corresponding to respective

rows of the database; and

encrypting all the row keys used in the second mode using

another key assigned commonly for the respective rows<u>;</u>

<u>wherein the item category titles identify respective</u>

15   <u>categories of the data segments</u>.

40.   (Currently Amended) A database management apparatus,

comprising:

a database storage unit which stores a database comprising a

plurality of records, each record including a plurality of data

-9-

5   segments identified by ~~respective~~ item <u>category</u> titles that

<u>identify respective categories of the data segments</u>;

an item <u>category</u> title memory for storing at least one item

<u>category</u> title for specifying a corresponding at least one data

segment group as a target of a data search process;

10   a key data memory for storing keys for use in encryption

associated with the database, wherein the keys comprise a column

key corresponding to said at least one data segment group

specified by the at least one stored item <u>category</u> title, and a

plurality of different row keys corresponding respectively to the

15   records of the database; and

an encryption unit for encrypting: (i) the data segments of

said at least one specified data segment group that is the target

of the data search process using the column key corresponding to

the at least one specified data segment group, and (ii) data

20   segments of at least one data segment group corresponding to item

<u>category</u> titles other than the at least one stored item <u>category</u>

title, in units corresponding to the records, using the different

row keys corresponding to the respective records and another

column key that is assigned commonly to the data segment groups

25   corresponding to item <u>category</u> titles other than the at least one

stored item <u>category</u> title.

-10-

41.   (Currently Amended) A computer program for directing a
computer to execute functions comprising:

accessing a database comprising a plurality of records, each
record including a plurality of data segments identified by

5   ~~respective~~ item category titles that identify respective

categories of the data segments;

storing at least one item category title for specifying a
corresponding at least one data segment group as a target of a
data search process;

10   storing keys for use in encryption associated with the
database, wherein the keys comprise a column key corresponding to
said at least one data segment group specified by the at least
one stored item category title, and a plurality of different row
keys corresponding respectively to the records of the database;

15   and

encrypting: (i) the data segments of said at least one
specified data segment group that is the target of the data
search process using the column key corresponding to the at least
one specified data segment group, and (ii) data segments of at

20   least one data segment group corresponding to item category
titles other than the stored item category titles, in units
corresponding to the records, using the different row keys of the
respective records.

-11-

42. (Currently Amended) A computer program for directing a
computer to execute functions comprising:

storing data specifying a type of encryption system to be
used to encrypt data segments of each column of a database, if

5   the column of the database is to be encrypted;

first encrypting in accordance with the data stored in the
key specification memory: (i) data segments forming data segment
groups corresponding to column item <u>category</u> titles of a first
kind using a same column key for said data segments forming the

10   data segment groups, and (ii) data segments forming data segment
groups corresponding to column item <u>category</u> titles of a second
kind, in units of rows of the database, using row keys
respectively specified for each of the rows<u>, said item category</u>
<u>titles identifying respective categories of the data segments</u>;

15   second encrypting, with a basic key, all the row keys; and

storing in a memory the database after the encryption
thereof and the row keys after encryption the encryption thereof,
in a mutually associated manner.

-12-